

1 What is claimed is:

2 1. A method for validating a user's authorization to run a tool in a service control manager (SCM)

3 module by a security manager, comprising:

4 obtaining a list of target nodes and a tool definition from a runnable tool;

5 obtaining the tool's roles from the tool definition;

6 checking if any of the tool's roles are enabled;

7 checking if the user is authorized on the nodes; and

8 checking if the user is authorized for at least one of the tool's enabled roles on the nodes.

9 2. The method of claim 1, wherein the obtaining the tool's roles step includes obtaining the tool's

10 roles, wherein the tool may be assigned one or more roles.

11 3. The method of claim 1, further comprising validating the roles.

12 4. The method of claim 1, further comprising obtaining the user's authorized roles for each node

13 in the list of target nodes from a hash table.

14 5. The method of claim 1, further comprising reporting whether the tool is runnable by the user.

15 6. The method of claim 5, wherein the reporting step includes reporting the tool as not runnable

16 by the user when all the roles are disabled.

17 7. The method of claim 5, wherein the reporting step includes reporting the tool as not runnable

18 by the user when the user is not authorized on each of the nodes.

19 8. The method of claim 5, wherein the reporting step includes reporting the tool as not runnable

20 by the user when the user is not authorized for any of the tool's enabled roles on all of the nodes.

21 9. A service control manager (SCM) module for validating a user's authorization to run a tool on

22 one or more target nodes, comprising:

23 target nodes that are managed servers;

24 tools that specify commands or options on the target nodes;

1 users that manage systems using the tools;
2 tools' enabled roles that are assigned to users to run the tools; and
3 a security manager that checks whether the user is authorized for one of the tools' enabled
4 roles.

5 10. The SCM module of claim 9, wherein the tools are single-system aware (SSA) tools.

6 11. The SCM module of claim 9, wherein the tools are multi-system aware (MSA) tools.

7 12. The SCM module of claim 9, wherein the target nodes can be target node groups.

8 13. A method for validating a user's authorization to run a tool in a service control manager (SCM)
9 module by a security manager, comprising:

10 obtaining a list of target nodes and tool definition from a runnable tool;

11 obtaining the tool's roles associated with the tool from the tool definition; and

12 checking if the user is authorized for one of the tool's roles on all of the nodes, wherein the user
13 assigned with the tool's roles on all of the nodes is authorized to run the tool.

14 14. The method of claim 13, wherein the obtaining the tool's roles step includes obtaining the tool's
15 roles, wherein the tool may be assigned one or more roles.

16 15. The method of claim 13, further comprising validating the roles.

17 16. The method of claim 13, further comprising obtaining the user's authorized roles for each node
18 in the list of target nodes from a hash table.

19 17. The method of claim 13, further comprising reporting whether the tool is runnable by the user.

20 18. The method of claim 17, wherein the reporting step includes reporting the tool as not runnable
21 by the user when all the roles are disabled.

22 19. The method of claim 17, wherein the reporting step includes reporting the tool as not runnable
23 by the user when the user is not authorized on each of the nodes.

24 20. The method of claim 17, wherein the reporting step includes reporting the tool as not runnable
25 by the user when the user is not authorized for any of the tool's enabled roles on all of the nodes.